



APPSEC
EUROPE





If You Can't Beat 'Em Join 'Em

Practical Tips For Running a Successful Bug Bounty Program

Grant McCracken
Shpend Kurtishaj

AppsecEU Rome
April 1, 2016



Grant

Technical Account Manager @Bugcrowd

(formerly an ASE)

Before that, Whitehat

Did some traveling

Music



Shpend

AppSec Engineer (ASE) @Bugcrowd

Team Lead

Bugbounty Hunter

Gamer



Bug Bounty Programs



wut



APPSEC
EUROPE

A (Brief) History of Bug Bounty Programs



Why?



Do you really want to let people attack you?



Source: http://hyperboleandahalf.blogspot.com/2010_06_01_archive.html



Yes! (They're doing it anyways...)



Source: http://hyperboleandahalf.blogspot.com/2010_06_01_archive.html



Who are these people?

All over the place!

All ages

All levels of experience

All over the world

Users and non-users

Passionate about security



Value

Lots of eyes

Only pay for valid results

Shows a more advanced security posture

Better overall reputation!



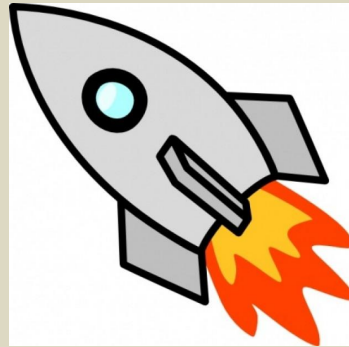
How?



How?

Pre-Launch

- Scope
- Focus
- Exclusions
- Environment
- Access



Post-Launch

- Managing Expectations
- Communicating Effectively
- Defining a Vulnerability Rating Taxonomy (VRT)



CASH MONEY
I'm gonna make it rain.

“Touch the code, pay the bug.”



You vs. and Them



Pre-Launch



Scope, scope, scope

Step 0...

Basic resources/requirements to run a program...

Scope defines the researcher's universe

Leave nothing open to interpretation
Understand your attack surface
The path of least resistance



Focus

You might care about specific:

Targets

Vuln types

Functionalities (e.g. payment processing)

How?

Incentives

Create a focused program



Source: <https://xkcd.com/1361/>



Exclusions

You might not care about:

- (Low-impact) “Low-hanging fruit”
- Intended functionality
- Known issues
- Accepted Risks
- Issues resulting from pivoting



Environment

Prod vs. Staging?

Make sure it can stand up to testing!

Scanners

Contact forms

Pentesting requests

Special bounty type? IoT?

Researcher environments?

**Not just a bigger display.
A bendable display.**

It's one thing to make a bigger display. It's something else entirely to make a bigger bendable display with brilliant colors and higher contrast at even extreme viewing angles. But that's exactly what we did with the new Retina HDB display.*



 *Viewing angles may vary from pocket to pocket



What a shared environment looks like...



Access

- Easier = better
- Provide researchers with the resources they'll need to be successful (e.g. credit cards, etc).
- No shared creds



Remember...



Post-Launch

- Be prepared
 - Triage Process
 - Communication
 - Vulnerability Rating Taxonomy
 - Horror Stories
 - Success Stories



\$UNPREPARED_COMPANY

Recipe for disaster:

Does not have human resources

Bad/Unclear exclusions

Don't provide known issues

Pays bad rewards



Triage Process

Reproduction Steps

Screenshots

Pocs

NOT Videos (without a supported writeup)



Triage Process

Good report

1. Go to url: <http://target.com>
2. Click on “button” x
3. Check burp for request z
4. Send to repeater
5. Modify param p to payload:
“><svg/onload=alert(1)
6. Send request
7. Browse <http://target.com/me.php> for
xss payload

Bad report

1. Login
2. Make the following request:
POST /suppliers/15 HTTP/1.1
...
3. XSS



Triage Process

Check Domain/Bug type if in scope

Check for duplicates

Replication Steps

Have accounts with diff roles ready

Have multiple browsers ready

Keep burp open (you'll need it)

Keep the scope handy

Rename valid bug titles



Communication is Key

Researchers like:

Concise, unambiguous responses

ESL

Quick responses

Predictable time to reward

Stay on top of these issues!



Define a Vulnerability Rating Taxonomy

For you:

- Speed up triage process
- Track your organization's posture
- Arrive at reward amount more quickly

For them (if published):

- Focus on high-value bugs
- Avoid reporting won't fix issues
- Feel a sense of trust (goes with brief)



Discuss the VRT at a Roundtable

Priority will change as your organization does.

Establish a discussion meeting to:

Review interesting bugs

Discuss additions to VRT

Propose changes to vulnerability classification/priorities

This is an ongoing process!



Horror Stories...



Diffie-Hellman (DH) key exchange parameters vurnavity

47.83% · [REDACTED] · 09/27/2015

Reference Number [REDACTED]

Bug Type SQL Injection

XSS Location URL Empty

Affected Parameter No FS 1 No SNI 2 TLS 1.0 TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa) No FS

Affected Users ALL

Attack String TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d) No FS

Browser Empty

Bug URL [REDACTED]

Device Empty

HTTP Request

```
Hello team [REDACTED]
I am Wamim , and I am here to report a vulnerability on your SITE!
Vuln[REDACTED]ity : Diffie-Hellman (DH) key exchange parameters

Severity:Medium/High.
Affected site:[REDACTED]
Here more information about the vulnerability and the impact: https://weakdh.org
Attack details/Proof of Concept by ssllabs.com(100% affidability)
Please, check the full scan here : https://www.ssllabs.com/ssltest/analyze.html?
```





XSS

Reference Number [REDACTED]

Bug Type XSS

XSS Location URL .js library

Affected Parameter update your .js library

Affected Users ALL

Attack String `$("${img src='x'>").on("error",function){alert(9)});`

Browser Empty

Bug URL [REDACTED]

Device Empty

HTTP Request

```
[REDACTED]
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:46.0) Gecko/20100101 Firefox/46.0
Accept: image/png,image/*;q=0.8,*/*;q=0.5
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: [REDACTED]
Cookie: [REDACTED]
Connection: close
Cache-Control: max-age=0
```

Method of Finding manual

Platform Empty

Platform Version Empty

Proof of Concept Empty

- Replication Steps
1. install firebug in your firefox
 2. execute this command in your console after the opening of the given link of your official page.

Tools Used fire bug



Horror Stories...

hello support ,

CSP header is missisng , that the CSP response headers served are missing , but the page without these headers can be cached by server. This makes it easier to mount a XSS attack or injuction attacks.

What is CSP?

Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware.

CSP is designed to be fully backward compatible; browsers that don't support it still work with servers that implement it, and vice-versa. Browsers that don't support CSP simply ignore it, functioning as usual, defaulting to the standard same-origin policy for web content. If the site doesn't offer the CSP header, browsers likewise use the standard same-origin policy.

Is there any Risk ?? Yeah ofcourse ,

The risk with CSP can have 2 main sources:

- 1] Policies misconfiguration,
- 2] Too permissive policies.



Horror Stories...

Cross-site request forgery, also known as a one-click attack or session riding and abbreviated as CSRF or XSRF, is a type of malicious exploit of a website whereby unauthorized commands are transmitted from a user that the website trusts

0% - [REDACTED] - 09/03/2015

Reference Number	[REDACTED]
Bug Type	CSRF
XSS Location URL	Empty
Affected Parameter	Empty
Affected Users	Empty
Attack String	Empty
Browser	Empty
Bug URL	www.google.sn/advanced_search www.google.sn/intl/fr/chrome/business/devices/tco.html www.google.sn/intl/fr/contact www.google.sn/intl/fr/edu/products/productivity-tools/classroom/index.html www.google.sn/intl/wo/contact www.google.sn/intx/wo/work/search/products/gss.html www.google.sn/movies www.google.sn/trends/explore
Device	Empty



Horror Stories...



Terms and Conditions missing severability clause

0% [REDACTED] 1/17/2015

Terms and Conditions missing sever ability clause.

Reference Number	[REDACTED]
Bug Type	Bug/Other
XSS Location URL	Empty
Affected Parameter	Empty
Affected Users	ALL
Attack String	Empty
Browser	Empty
Bug URL	[REDACTED]com/terms
Device	Empty
HTTP Request	null
Method of Finding	[REDACTED]com/terms



Success Stories

Instructure

	2013 (Pentest)	2014 (Bug Bounty)
Critical	0	0
High	1	25
Medium	1	8
Low	2	16

Source: <https://www.canvaslms.com/security>



tl;dr



WHY DO WHALES JUMP
WHY ARE WITCHES GREEN
WHY ARE THERE MIRRORS ABOVE BEDS
WHY DO I SAY UH
WHY IS SEA SALT BETTER
WHY ARE THERE TREES IN THE MIDDLE OF FIELDS
WHY IS THERE NOT A POKEMON MMO
WHY IS THERE LAUGHING IN TV SHOWS
WHY ARE THERE DOORS ON THE FREEWAY
WHY ARE THERE SO MANY SUICIDE CASES RUNNING
WHY AREN'T THERE ANY COUNTRIES IN ANTARCTICA
WHY ARE THERE SCARY SOUNDS IN MINECRAFT
WHY IS THERE KICKING IN MY STOMACH
WHY ARE THERE TWO SLASHES AFTER HTTP
WHY ARE THERE CELEBRITIES
WHY DO SNAKES EXIST
WHY DO OYSTERS HAVE PEARLS
WHY ARE DUCKS CALLED DUCKS
WHY DO THEY CALL IT THE CLAP
WHY ARE KYLE AND CARTMAN FRIENDS
WHY IS THERE AN ARROW ON PANG'S HEAD
WHY ARE TEXT MESSAGES BLUE
WHY ARE THERE MUSTACHES ON CARS
WHY ARE THERE MUSTACHES EVERYWHERE
WHY ARE THERE SO MANY BIRDS IN OHIO
WHY IS THERE SO MUCH RAIN IN OHIO
WHY IS OHIO WEATHER SO WEIRD
WHY ARE THERE MALE AND FEMALE BIKES
WHY ARE THERE UNIVERSITY'S
WHY DO LIVING PEOPLE RESEARCH UP
WHY AREN'T THERE UNUSUAL FRIENDS
WHY ARE OLD KINGDOMS DIFFERENT

WHY DO TESTICLES MOVE
WHY ARE THERE PSYCHICS
WHY ARE HATS SO EXPENSIVE
WHY IS THERE COFFEINE IN MY SHAPPOO
WHY DO YOUR BOOBS HURT
WHY DO TWINNS DIE
WHY AREN'T ECONOMISTS RICH
WHY DO AMERICANS CALL IT SOCCER
WHY ARE MY EARS RINGING
WHY ARE THERE SO MANY AVENGERS
WHY ARE THE AVENGERS FIGHTING THE X MEN
WHY IS WOLVERINE NOT IN THE AVENGERS
WHY AREN'T THERE DINOSAURS
WHY ARE THERE TINY SPIDERS IN MY HOUSE
WHY DO SPIDERS COME INSIDE
WHY ARE THERE HUGE SPIDERS IN MY HOUSE
WHY ARE THERE LOTS OF SPIDERS IN MY HOUSE
WHY ARE THERE SPIDERS IN MY ROOM
WHY ARE THERE SO MANY SPIDERS IN MY ROOM
WHY DO SPIDER BITES ITCH
WHY IS DYING SO SCARY
WHY IS THERE NO GPS IN LAPTOPS
WHY DO KNEES CLICK
WHY AREN'T THERE E GRADUES
WHY IS ISOLATION BAD
WHY DO BOYS LIKE ME
WHY DON'T BOYS LIKE ME
WHY IS THERE ALWAYS A TARA UPRITE
WHY ARE THERE RED DOTS ON MY BREASTS
WHY IS LYING GOOD

WHY ARE THERE SLAVES IN THE BIBLE
WHY IS HTTPS CROSSED OUT IN RED
WHY IS THERE A LINE THROUGH HTTPS
WHY IS THERE A RED LINE THROUGH HTTPS ON FACEBOOK
WHY IS HTTPS IMPORTANT
WHY AREN'T MY ARMS GROWING
WHY ARE THERE CROWS IN ROCHESTER
WHY ARE THERE PSYCHIC WEAK TO BUG
WHY DO CHILDREN GET CANCER
WHY IS POSEIDON ANGRY WITH ODYSSEUS
WHY IS THERE ICE IN SPACE
WHY ARE DOGS AFRAID OF FIREWORKS
WHY IS THERE NO KING IN ENGLAND
WHY ARE THERE OWLS IN MY BACKYARD
WHY IS THERE AN OWL OUTSIDE MY WINDOW
WHY IS THERE AN OWL ON THE DOLLAR BILL
WHY DO OWLS ATTACK PEOPLE
WHY ARE AK 47s SO EXPENSIVE
WHY ARE THERE HELICOPTERS CIRCLING MY HOUSE
WHY ARE THERE GODS
WHY ARE THERE TWO SPOOKS
WHY ARE MY BOOBS ITCHY
WHY ARE CIGARETTES LEGAL
WHY ARE THERE DUCKS IN MY POOL
WHY IS JESUS WHITE
WHY IS THERE LIQUID IN MY EAR
WHY DO Q TIPS FEEL GOOD
WHY DO GOOD PEOPLE DIE
WHY IS LIFE SO BORING
WHY AREN'T THERE GUNS IN HARRY POTTER
WHY ARE ULTRASOUNDS IMPORTANT
WHY ARE ULTRASOUND PAINED EXPENSIVE
WHY IS STEALING WRONG
WHY AREN'T THERE ANY FOREIGN MILITARY BASES IN AMERICA

WHY ARE THERE ZIPPER
WHY ARE THERE PHLEGM
WHY ARE THERE LAMAS
WHY ARE THERE PHLEGM
WHY ARE THERE LAMAS

WHY ARE THERE GHOSTS
WHY ARE THERE FEMALE MR NIMMES

WHY IS SEX SO IMPORTANT

WHY ARE THERE GHOSTS

WHY ARE THERE FEMALE MR NIMMES

WHY AREN'T MY ARMS GROWING






WHY AREN'T THERE GUNS IN HARRY POTTER

WHY ARE ULTRASOUNDS IMPORTANT
WHY ARE ULTRASOUND PAINED EXPENSIVE
WHY IS STEALING WRONG

WHY AREN'T MY QUAIL LAYING EGGS
WHY AREN'T MY QUAIL EGGS HATCHING
WHY AREN'T THERE ANY FOREIGN MILITARY BASES IN AMERICA

QUESTIONS

FOUND IN GOOGLE AUTOCOMPLETE

Source: <https://xkcd.com/1256/>



APPSEC EUROPE